In the Abstract:

ABSTRACT OF THE DISCLOSURE

~~A METHOD AND APPARATUS FOR ANONYMOUS SIGNATURE BY MEANS OF A SHARED PRIVATE KEY~~

~~The invention concerns a~~ A cryptographic method and apparatus for anonymously signing a message. ~~The method consists in adding~~ Added to the anonymous signature is another ~~an additional~~ signature which is calculated (operation 13) using a private key common to all the members of a group authorized to sign and unknown to all revoked members. ~~Said~~ The private key is updated (operations 8, 11) at group level on each revocation within the group and at member level only on anonymous signing of a message by the member. ~~The apparatus comprises as many smart cards as there are members in the group and apparatus comprising first calculating means.~~